Nathan R. Ring
Nevada State Bar No. 12078
STRANCH, JENNINGS & GARVEY, PLLC
3100 W. Charleston Blvd., Ste. 208
Las Vegas, NV 89102
Telephone: 725-235-9750
E-mail: LasVegas@StranchLaw.com

Maureen M. Brady MO #57800
(pro hac vice petition forthcoming)
MCSHANE & BRADY, LLC
1656 Washington Street, Suite 120
Kansas City, MO 64108
Telephone: (816) 888-8010
Facsimile: (816) 332-6295
E-mail: mbrady@mcshanebradylaw.com

Sharon J. Zinns, Esq.
(pro hac vice petition forthcoming)
Georgia Bar No. 552920
ZINNS LAW, LLC
4243 Dunwoody Club Drive, Suite 104
Atlanta, GA 30350
(404) 882-9002
sharon@zinnslaw.com

Attorneys for Plaintiffs

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEVADA

DAVID ZUSSMAN, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

VICI PROPERTIES L.P., a Delaware limited partnership; VICI PROPERTIES 2 L.P., a Delaware limited partnership; MGM RESORTS INTERNATIONAL, a Delaware corporation; and MGM GROWTH PROPERTIES OPERATING PARTNERSHIP L.P., a Delaware limited

Case No.:
Dept. No:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

liability company,

Defendants.

CLASS ACTION COMPLAINT

COMES NOW Plaintiff David Zussman, individually and on behalf of all others similarly situated, and on behalf of the general public, upon personal knowledge of facts pertaining to him and upon information and belief as to all other matters, and by and through undersigned counsel, hereby brings this Class Action Complaint against Defendants VICI Properties L.P., VICI Properties 2 L.P., MGM Resorts International, and MGM Growth Properties Operating Partnership L.P. (hereinafter "Defendants" and/or "MGM") and alleges as follows:

INTRODUCTION

1. Plaintiff brings this action on behalf of himself and all other individuals similarly situated ("Class Members") against Defendants for their failure to secure and safeguard the personally identifiable information ("PII") of several million individuals, whose information constituted 6 terabytes of information,[1] who are customers of Defendants.

2. VICI Properties L.P., (otherwise known as "MGM") is incorporated in Delaware with its principal place of business at 3600 South Las Vegas Blvd., Las Vegas, NV 89109. It is an entertainment company, consisting of casinos, restaurants, hotels, and various other entertainment ventures. In the regular course of its business, MGM is required to maintain reasonable and adequate security measures to secure, protect, and safeguard their customers' PII against unauthorized access and disclosure.

3. VICI Properties 2 L.P., (otherwise known as "MGM") is incorporated in Delaware with its principal place of business at 3600 South Las Vegas Blvd., Las Vegas, NV

[1] https://www.reuters.com/technology/hackers-who-breached-casino-giants-mgm-caesars-also-hit-3-other-firms-okta-says-2023-09-19/ (Last visited September 19, 2023).

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

89109. It is an entertainment company, consisting of casinos, restaurants, hotels, and various other entertainment ventures. In the regular course of its business, MGM is required to maintain reasonable and adequate security measures to secure, protect, and safeguard their customers' PII against unauthorized access and disclosure.

4. MGM Resorts International, (otherwise also known as "MGM") is incorporated in Delaware with its principal place of business at 3600 South Las Vegas Blvd., Las Vegas, NV 89109. It is an entertainment company, consisting of casinos, restaurants, hotels, and various other entertainment ventures. In the regular course of its business, MGM is required to maintain reasonable and adequate security measures to secure, protect, and safeguard their customers' PII against unauthorized access and disclosure.

5. MGM Growth Properties Operating Partnership LP (otherwise known as "MGM") headquartered in Wilmington, Delaware, is an entertainment company, consisting of casinos, restaurants, hotels, and various other entertainment ventures. In the regular course of its business, MGM is required to maintain reasonable and adequate security measures to secure, protect, and safeguard their customers' PII against unauthorized access and disclosure.

6. Every year, millions of Americans have their most valuable PII stolen and sold online because of data breaches. Despite the dire warnings about the severe impact of data breaches on Americans of all economic strata, companies, including Defendants, still fail to make the necessary investments to implement important and adequate security measures to protect their customers' and employees' data.

7. Defendants required their customers to provide them with their sensitive PII and failed to protect it. Defendants had an obligation to secure their customers' PII by implementing

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

reasonable and appropriate data security safeguards. This was part of the bargain between Plaintiff and Class Members and Defendants.

8. As reported by Defendants, hackers ALPHV and Scattered Spider a.k.a. UNC 3944 found their way into Defendants' systems, stealing both former and current customer names, birth dates, Social Security numbers, credit history, and drivers' license information of Defendants' customers (the "Data Breach").

9. Defendants required their customers to provide them with their sensitive PII and failed to protect it. Defendants had an obligation to secure their customers' PII by implementing reasonable and appropriate data safeguards. This was part of the bargain between Plaintiff and Class Members and Defendants.

10. As a result of Defendants' failure to provide reasonable and adequate data security, Plaintiff's and the Class Members' unencrypted, non-redacted PII has been exposed to unauthorized third parties. Plaintiff and the Class are now at much higher risk of identity theft and cybercrimes of all kinds, especially considering the highly sensitive PII stolen here and the fact that the compromised PII is already being sold on the dark web. This risk constitutes a concrete injury suffered by Plaintiff and the Class as they no longer have control over their PII, which PII is now in the hands of third-party cybercriminals. This substantial and imminent risk of identity theft has been recognized by numerous courts as a concrete injury sufficient to establish standing.

11. Plaintiff and the Class will have to incur costs to pay a third-party credit and identity theft monitoring service for the rest of their lives as a direct result of the Data Breach.

12. Plaintiff brings this action on behalf of himself and those similarly situated to seek redress for the lifetime of harm they will now face, including, but not limited to, reimbursement of losses associated with identity theft and fraud, out-of-pocket costs incurred to

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

mitigate the risk of future harm, compensation for time and effort spent responding to the Data Breach, the costs of extending credit monitoring services and identity theft insurance, and injunctive relief requiring Defendants to ensure that their third-party vendors implement and maintain reasonable data security practices going forward.

THE PARTIES

13. Plaintiff David Zussman is a resident of Lakeway, Travis County, Texas, whose Personal Information was compromised in the Data Breach.

14. Defendant VICI Properties L.P. is a Delaware limited partnership, having a foreign corporation in Nevada, with its principal place of business at 3600 South Las Vegas Blvd., Las Vegas, NV 89109. It can be served through its registered agent: Corporation Service Company, 112 N Curry St., Carson City, NV 89703. VICI Properties L.P. is the parent company to MGM.

15. Defendant VICI Properties 2 L.P. is a Delaware limited partnership, with authorization to conduct business as a foreign corporation in Nevada, with its principal place of business at 3600 South Las Vegas Blvd., Las Vegas, NV 89109. It can be served through its registered agent: Corporation Service Company, 112 N Curry St., Carson City, NV 89703. VICI Properties is the parent company to MGM.

16. Defendant MGM Resorts International is a Delaware corporation, with authorization to conduct business as a foreign corporation in Nevada. Its principal place of business is at 3600 South Las Vegas Blvd., Las Vegas, NV 89109. It can be served through its registered agent: Corporation Service Company, 112 North Curry St., Carson City, NV 89703.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
SJG STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

17. Defendant MGM Growth Properties Operating Partnership L.P. is a Delaware limited partnership and can be served through its registered agent: Corporation Service Company, 251 Little Falls Dr., Wilmington, DE 19808.

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §1332(d) because there are more than 100 Class Members, at least one class member is a citizen of a state different from that of Defendants, and the amount in controversy exceeds $5 million, exclusive of interest and costs.

19. Venue is likewise proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendants conduct much of their business in this District and Defendants have caused harm to Class Members residing in this District.

GENERAL ALLEGATIONS COMMON TO ALL COUNTS

20. This is a class action brought by Plaintiff, individually and on behalf of all citizens who are similarly situated (i.e., the Class Members), seeking to dress Defendants' willful and reckless and violations of his privacy rights. Plaintiff and the other Class Members were customers of Defendants.

21. On or about August 1, 2023 through September 19, 2023, unauthorized third parties ALPHV and Scattered Spider (aka UNC 3944) accessed and downloaded Plaintiff's and the Class Members' PII.

22. This action pertains to Defendants' unauthorized disclosures of the Plaintiff's PII that occurred between August 1, 2023 and September 19, 2023.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
SJG STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

23. Plaintiff is a member of the MGM Rewards loyalty program, which allows members to, "earn rewards for your hotel stays, dining, slots, table games, and more. Then redeem your MGM Rewards points to do it all over again, on [Defendants]."[2]

24. As a condition of receiving their products and/or services, Defendants require that consumers and/or members of their MGM Rewards program, including Plaintiff and Class members, trust it with highly sensitive personal information.

25. In order to obtain an MGM Rewards membership, Plaintiff was required to provide their PII to Defendants, including his name, date of birth, contact information, drivers' license information, Social Security Number, and credit history.

26. Defendants disclosed Plaintiff's and the other Class Members' PII to unauthorized persons as a direct and/or proximate result of Defendants' failure to safeguard and protect their PII.

27. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendants assumed legal and equitable duties and knew or should have known it was responsible for protecting the PII from unauthorized disclosures.

28. MGM states, "Information maintained in electronic form that is collected by MGM Resorts International and any individual MGM Resort is stored on systems protected by industry standard security measures. These security measures are intended to protect these systems from unauthorized access." "Our staff is required to take reasonable measures to ensure that unauthorized persons cannot view or access your Personal Information."[3]

29. Despite recognizing their duty to do so, Defendants failed to assess and monitor their security safeguards to protect Plaintiff's and the Class Members' PII.

[2] https://www.mgmresorts.com/en/mgm-rewards.html (Last visited September 25, 2023).
[3] https://www.mgmresorts.com/en/privacy-policy.html (Last visited on September 19, 2023).

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

30. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendants to keep their PII confidential and maintained securely, to use this information for business purposes only, to make only authorized disclosures of this information, and to ensure that their third-party vendors take similar steps.

The Data Breach

31. According to a data breach notice sent by Defendants ("Breach Notice"), an unauthorized party accessed one of MGM's transfer servers from August 1, 2023 through September 19, 2023, exploiting a glaring vulnerability in the software and downloading highly sensitive PII of thousands of MGM customers stored on its servers including Social Security numbers, first and last names, dates of birth, zip codes, drivers' license information, and credit history information.

32. The Breach Notice further provided that, "A security incident has surfaced." And that, "[h]ackers admit to stealing 6 terabytes of data from popular casinos, MGM Resorts and Caesars Entertainment."

33. Absent from the Breach Notice are any details regarding how the Data Breach happened, what Defendants did in response to the ransom demand, or how Defendants' actions have remediated the root cause of the Data Breach.

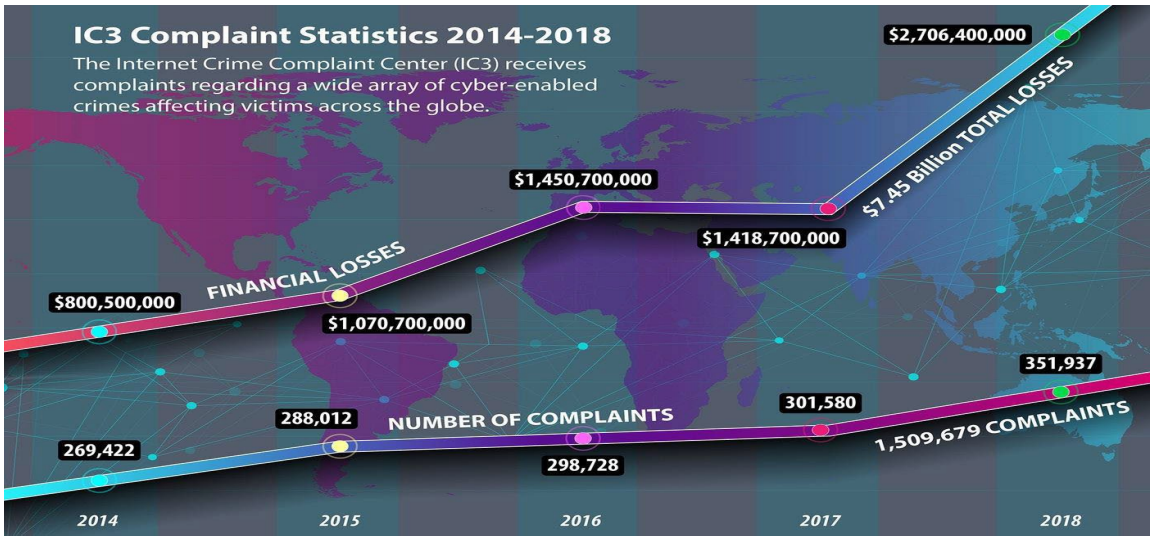
The Data Breach was Preventable

34. Had Defendants insured that they maintained industry-standard safeguards to monitor, assess, and update security controls and related system risks, they could have ensured sensitive customer data was not transferred to a vendor that was unequipped to protect it. Defendants' lack of oversight of their security controls, and their implementation of enhanced security measures only after the Data Breach are inexcusable.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

35. Defendants were at all times fully aware of their obligation to protect their customers' PII and the risks associated with failing to do so. Defendants observed frequent public announcements of data breaches affecting finance and insurance industries and knew that information of the type collected, maintained, and stored by Defendants is highly coveted and a frequent target of hackers.

36. This exposure, along with the fact that the compromised PII is potentially already being sold on the dark web, is tremendously problematic. Cybercrime is rising at an alarming rate, as shown in the FBI's Internet Crime Complaint statistics chart shown below:



37. By 2013, it was being reported that nearly one out of four data breach notification recipients becomes a victim of identity fraud.[4]

38. Stolen PII is often trafficked on the dark web. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

[4] Pascual, Al, "2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters," *Javelin* (Feb. 20, 2013).

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

39. When malicious actors infiltrate companies and copy and exfiltrate the PII that those companies store, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[5]

40. In April 2023, NationsBenefits, "disclosed that thousands of its members had their personal information compromised in a late-January ransomware attached targeting Fortra's Anywhere platform, a file-transfer software that the firm was using. According to the news reports, the ransomeware gang CLOP claimed responsibility for the attack, saying it took advantage of a previously known vulnerability."[6]

41. In mid-April 2023, "the second largest health insurer [Point32Health], in Massachusetts, suffered major technical outages resulting from a ransomware attack. The incident brought down the company's systems that it uses to service members and providers, resulting in some members having difficulty contacting their insurers."[7]

42. In May 2023, MCNA Insurance Company disclosed that "personal health information of nearly nine million patients was compromised in a cyber incident discovered in March. In a data breach notification letter filed with the Maine state attorney general's office dated May 26, the firm said that it detected unauthorized access to its systems on March 6, with some found to be infected with malicious code…According to MCNA, the hackers were successful in accessing patient personal information."[8]

43. In April 2020, ZDNet reported in an article titled, "Ransomeware mentioned in 1,000+ SEC filings over the past year", that "[r]ansomeware gangs are now ferociously

[5] *Shining a Light on the Dark Web with Identity Monitoring*, IdentityForce, Dec. 28, 2020, *available at:* https://www.identityforce.com/blog/shining-light-dark-web-identity- monitoring (last accessed July 28, 2021).

[6] https://www.insurancebusinessmag.com/us/guides/the-insurance-industry-cyber-crime-report-recent-attacks-on-insurance-businesses-448429.aspx (Last visited August 22, 2023)

[7] *Id.*

[8] *Id.*

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news complaints as revenge against those who refuse to pay."[9]

44. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomeware Guide" advising that "[m]alicious actors have adjusted their ransomeware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[10]

45. Another example is when the U.S. Department of Justice announced its seizure of AlphaBay in 2017. AlphaBay had more than 350,000 listings, many of which concerned stolen and fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PII] belonging to victims from countries all over the world. One of the key challenges of protecting PII online is its pervasiveness. As data breaches in the news continue to show, PII about employees, customers, and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[11]

46. The PII of consumers remains of high value to criminals, as evidenced by the price they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to

[9] https://www.zdnet.com/article/ransomeware-mentioned-in-1000-sec-filings-over-the-past-year/ (Last visited August 22, 2023).

[10] https://www.cisa.gov/sites/default/files/2023-01-CISA_MS-ISAC_Ransomware%20Guide_8508C.pdf (Last visited August 22, 2023).

[11] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor, April 3, 2018, *available at:* https://www.armor.com/resources/blog/stolen-pii-ramifications- identity-theft-fraud-dark-web/ (Last visited July 28, 2021).

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

$200, and bank details have a price range of $50 to $200.[12] Experian reports that a solen credit or debit card number can sell for $5 to $110 on the dark web.[13] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[14]

47. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number assuming your identity can cause a lot of problems.[15]

48. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventative action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraudulent activity to obtain a new number.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

[12] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal- data-sold-on-the-dark-web-how-much-it-costs/ (Last visited July 28, 2021).
[13] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask- experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (Last visited July 28, 2021).
[14] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the- dark/ (Last visited July 28, 2021).
[15] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (Last visited August 22, 2023).

49. Even then, a new Social Security number may not be effective. According to July Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[16]

50. Because of this, the information comprised in the Data Breach here is significantly more harmful to lose than the loss of, for example, credit card information in a retailer payment card breach because victims can simply cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

51. The PII compromised in the Data Breach demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[17]

52. Once PII is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends, and colleagues of the original victim.

53. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.

[16] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen- by-anthem-s-hackers-has-millionsworrying- about-identity-theft (last visited July 28, 2021).

[17] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells- for- 10x-price-of-stolen-credit-card-numbers.html (last visited July 28, 2021).

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

54. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

55. Data breaches facilitate identity theft as hackers obtain consumers' PII and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII to others who do the same.

56. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PII to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[18] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will fact, "substantial costs and inconveniences repairing damage to their credit records… [and their] good name."[19]

57. The exposure of Plaintiff's and Class Members' PII to cybercriminals will continue to cause substantial risk of future harm, including identity theft, that is continuing and imminent in light of the many different avenues of fraud and identity theft utilized by third-party cybercriminals to profit off this highly sensitive information.

Defendants Failed to Comply with the Federal Trade Commission

58. Federal and State governments have established security standards and issued recommendations to minimize data breaches and the resulting harm to individuals and financial

[18] *See* Government Accountability Office, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), https://www.gao.gov/assets/gao- 07-737.pdf (last visited July 28, 2021).
[19] *Id.*

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[20]

59. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business,* which established guidelines for fundamental data security principals for business.[21] Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted form the system; and have a response plan ready in the event of a breach.[22]

60. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[23]

61. Highlighting the importance of protecting against phishing and other types of data breaches, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, treating the failure to employ reasonable and appropriate

[20] *See* Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain- language/pdf0205-startwithsecurity.pdf (last visited July 28, 2021).

[21] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited August 22, 2023).

[22] *Id.*

[23] Federal Trade Commission, *Start With Security*, *supra footnote 17*.

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

The Impact of Data Breach on Victims

62. Defendants' failure to keep Plaintiff's and Class Members' PII secure has severe ramifications. Given the highly sensitive nature of the PII stolen in the Data Breach, Social Security numbers, first and last names, and dates of birth, hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiff and Class Members now and into the indefinite future. As a result, Plaintiff has suffered injury and faces an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach.

63. The PII exposed in the Data Breach is highly coveted and valuable on underground markets. Identity thieves can use the PII to: (a) commit insurance fraud; (b) obtain a fraudulent driver's license or ID card in the victim's name; (c) obtain fraudulent government benefits; (d) file a fraudulent tax return using the victim's information; (e) commit medical and healthcare-related fraud; (f) access financial and investment accounts and records; (g) engage in mortgage fraud; and/or (h) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest.

64. Further, malicious actors often wait months or years to use the PII obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen PII, meaning individuals can be victims of several cybercrimes stemming from a single data breach.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

65. Given the confirmed exfiltration of Defendants' customers' PII from their servers, many victims of the Data Breach have likely already experienced significant harms as the result of the Data Breach, including, but not limited to, identity theft and fraud. Plaintiff and Class Members have also spent time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit monitoring services, reviewing financial and insurance statements, checking credit reports, and spending time and effort searching for unauthorized activity.

66. It is no wonder, then, that identity theft exacts a severe emotional toll on its victims. The 2021 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft:

- 84% reported anxiety;
- 76% felt violated;
- 32% experienced financial related identity problems;
- 83% reported being turned down for credit or loans;
- 32% reported problems with family members as a result of the breach;
- 10% reported feeling suicidal.[24]

67. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48% reported sleep disturbances;
- 37.1% reported an inability to concentrate/lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;

[24] https://www.idtheftcenter.org/wp-content/uploads/2021/09/ITRC_2021_Consumer_Aftermath_Report.pdf (Last visited August 22, 2023).

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

- 23.1 reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[25]

68. Annual monetary losses from identity theft are in the billions of dollars. According to a Presidential Report on identity theft produced in 2007:

> In addition to the losses that result when identity thieves fraudulently open accounts…individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

69. The unauthorized disclosure of sensitive PII to data thieves also reduces its inherent value to its owner, which has been recognized by courts as an independent form of harm.[26]

70. Consumers are injured every time their data is stolen and/or traded on underground markets, even if they have been victims of previous data breaches. Indeed, the dark web is comprised of multiple discrete repositories of stolen information that can be aggregated together or accessed by different criminal actors who intent to use it for different fraudulent

[25] *Id.*

[26] *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—that the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information.
Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

purposes. Each data breach increases the likelihood that a victim's personal information will be exposed to more individuals who are seeking to misuse it at the victim's expense.

71. As a result of the wide variety of injuries that can be traced to the Data Breach, Plaintiff and Class Members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. The unconsented disclosure of confidential information to a third party;

b. Unauthorized use of their PII without compensation;

c. Losing the value of the explicit and implicit promises of data security;

d. Losing the value of access to their PII permitted by Defendants without their permission;

e. Identity theft and fraud resulting from the theft of their PII;

f. Costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

g. Anxiety, emotional distress, and loss of privacy;

h. The present value of ongoing credit monitoring and identity theft protection services necessitated by the Data Breach;

i. Unauthorized charges and loss of use of and access to their accounts;

j. Lowered credit scores resulting from credit inquiries following fraudulent activities;

k. Costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including searching for fraudulent activity, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and

l. The continued, imminent, and certainly impending injury flowing from potential fraud and identity theft posed by their PII being in the possession of one or more unauthorized third parties.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

72. Even in instances where an individual is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement. The Department of Justice's Bureau of Justice Statistics found that identity theft victims, "reported spending an average of about 7 hours clearing up the issues" relating to identity theft or fraud.[27]

73. Plaintiff and Class Members place significant value in data security. According to a survey conducted by cyber-security company FireEye Mandiant, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more to work with a provider that has better data security. Seventy percent of consumers would provide less personal information to organizations that suffered a data breach.[28]

74. Plaintiff and Class Members have a direct interest in Defendants' promises and duties to protect their PII, i.e., that Defendants *not increase* their risk of identity theft and fraud. Because Defendants failed to live up to their promises and duties in this respect, Plaintiff and Class Members seek the present value of ongoing identity protection services to compensate them for the present harm and present and continuing increased risk of harm caused by Defendants' wrongful conduct. Through this remedy, Plaintiff seeks to restore themselves and Class Members as close to the same position as they would have occupied but for Defendants' wrongful conduct, namely their failure to adequately protect Plaintiff's and the Class Members' PII.

75. Plaintiff and Class Members further seek to recover the value of the unauthorized access to their PII permitted through Defendants' wrongful conduct. This measure of damages is

[27] E. Harrell, U.S. Department of Justice, *Victims of Identity Theft, 2014* (revised Nov. 14, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf (Last visited August 22, 2023).

[28] https://web.archive.org/web20220205174527/https://www.fireeye.com/blog/executive-perspective/2016/05/beyong_the_bottomli.html (Last visited August 15, 2023).

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

analogous to the remedies for the unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a person's PII is non-rivalrous—the unauthorized use by. Another does not diminish the rights-holder's ability to practice the patented invention or use the trade-secret protected technology. Nevertheless, a Plaintiff may generally recover the reasonable use of the value of the IP—i.e., a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the owner's own use (as in the case of a nonpracticing patentee) and even though the owner would not have otherwise licensed such IP to the infringer. A similar royalty or license measure of damages is appropriate here under common law damages principles authorizing recovery of rental or use value. This measure is appropriate because: (a) Plaintiff and Class Members have a protectible property interest in their PII; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; (c) rental value is established with reference to market value, i.e., evidence regarding the value of similar transactions.

76. Plaintiff and Class Members have an interest in ensuring their PII is secured and not subject to further theft because Defendants continues to hold their PII.

CLASS ACTION ALLEGATIONS

77. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of himself and the following proposed Nationwide class, defined as follows:

Nationwide Class

All persons residing in the United States who are current or former customers of MGM or any MGM affiliate, parent, or subsidiary, and had their PII compromised by an unknown third-party cybercriminal as a result of the Data Breach.

In addition, Plaintiff brings this action on behalf of the following proposed Texas Subclass, defined as follows:

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

Texas Subclass

All persons residing in the State of Texas who are current or former customers of MGM or any MGM affiliate, parent, or subsidiary, and had their PII compromised by an unknown third-party cybercriminal as a result of the Data Breach.

78. Both the proposed Nationwide Class and the proposed Texas Subclass will be collectively referred to as the Class, except where it is necessary to differentiate them.

79. Excluded from the proposed Class are any officer or director of Defendant; any officer or director of any affiliate, parent, or subsidiary of MGM, or anyone employed by counsel in this action; and any judge to whom this case is assigned, his or her spouse, and members of the judge's staff.

80. **Numerosity.** Members of the proposed Class likely number in the tens of thousands and are thus too numerous to practically join in a single action. Membership in the Class is readily ascertainable from Defendants' own records.

81. **Commonality and Predominance.** Common questions of law and fact exist as to the proposed Class Members and predominate over questions affecting only individual Class Members. These common questions include:

a. Whether Defendants engaged in the wrongful conduct alleged herein;

b. Whether Defendants' inadequate data security measures were a cause of the Data Breach;

c. Whether Defendants owed a legal duty to Plaintiff and the other Class Members to exercise due care in collecting, storing, and safeguarding their PII;

d. Whether Defendants negligently or recklessly breached legal duties owed to Plaintiff and the Class Members to exercise due care in collecting, storing, and safeguarding their PII;

e. Whether Plaintiff and the Class are at an increased risk for identity theft because of the Data Breach;

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

f. Whether Defendants failed to implement and maintain reasonable security procedures and practices for Plaintiff's and Class Members' PII in violation of Section 5 of the FTC Act;

g. Whether Plaintiff and the other Class Members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

82. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, individually, and on behalf of the other Class Members. Similar or identical statutory and common violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

83. **Typicality:** Plaintiff's claims are typical of the claims of the Members of the Class. All Class Members were subject to the Data Breach and had their PII accessed by and/or disclosed to unauthorized third parties. Defendants' misconduct affected all Class Members in the same manner.

84. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because their interests do not conflict with the interests of the other Class Members they seek to represent; they have retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and their counsel.

85. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the other Class Members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendants, making it impracticable for Class Members to individually

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

seek redress for Defendants' wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

COUNT I
OUTRAGEOUS CONDUCT
(On behalf of Plaintiff and the Texas Subclass)

86. Plaintiff and the other Class Members incorporate by reference the allegations of the foregoing paragraphs as though set forth fully herein.

87. At all times relevant hereto, Defendants owe a duty to Plaintiff and the other Class Members to keep their customers' PII private, and not reveal PII to third parties without first obtaining the customer's expressed consent.

88. Defendants disclosed Plaintiff's and other Class Members' highly sensitive PII to the public either intentionally or with reckless disregard for Plaintiff and the other Class Members.

89. Defendants' conduct was extreme and outrageous and caused Plaintiff and the other Class Members extreme and severe mental distress.

90. As a direct result of Defendants' actions Plaintiffs suffered harms, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, increased infiltrations into their privacy through spam and/or attempted identity theft, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation, and loss of enjoyment of life.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

COUNT II
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Nationwide Class or, alternatively, the Texas Subclass)

91. The preceding factual statements and allegations are incorporated herein by reference.

92. Plaintiff and the other Class Members, as part of their agreement with Defendants, provided Defendants their PII.

93. Defendants offered products and services to current or former customers, including Plaintiff and Class Members, in exchange for monetary payment.

94. As a condition of the purchase, Defendants required Plaintiff and Class Members to provide their PII, including names, addresses, dates of birth, Social Security numbers, driver's license numbers, credit history, and other personal information. Implied in these exchanges was a promise by Defendants to ensure that the PII of Plaintiff and Class Members in their possession was only used to provide the agreed-upon products and services from Defendants.

95. These exchanges constituted an agreement between the parties: Plaintiff and Class Members would provide their PII in exchange for the products and services provided by Defendants.

96. It is clear by these exchanges that the parties intended to enter into an agreement. Plaintiff and Class Members would not have disclosed their PII to Defendants but for the prospect of Defendants' promise of providing the products and services purchased by Plaintiff and the Class. Conversely, Defendants presumably would not have taken Plaintiff's and Class Members' PII if it did not intend to provide Plaintiff and Class Members with the bargained-for products and services.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

97. In providing such PII, Plaintiff and the other Class Members entered into an implied contract with Defendants, whereby Defendants became obligated to reasonably safeguard Plaintiff's and the other Class members' PII.

98. Under the implied contract, Defendants were obligated to not only safeguard the PII, but also to provide Plaintiff and Class Members with prompt, adequate notice of any Data Breach or unauthorized access of said information.

99. Defendants breached the implied contract with Plaintiff and the other Class Members by failing to take reasonable measures to safeguard their PII.

100. As a direct result of Defendants' breach of their duty of confidentiality and privacy and the disclosure of Plaintiff's and the member of the Class confidential information, Plaintiff and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, increased infiltrations into their privacy through spam and/or attempted identity theft, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

101. Plaintiff and the other Class Members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiff and Class Members are entitled to nominal damages.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

COUNT III
NEGLIGENCE
(On behalf of Plaintiff and the Nationwide Class or, alternatively, the Texas Subclass)

102. The preceding factual statements and allegations are incorporated herein by reference.

103. Defendants owed a duty to Plaintiff and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiff's and Class Members' PII from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, maintaining, and testing their data security systems to ensure that Plaintiff's and Class Members' PII in Defendants' possession was adequately secured and protected.

104. Defendants owed, and continue to owe, a duty to Plaintiff and the other Class Members to safeguard and protect their PII.

105. Defendants breached their duty by failing to exercise reasonable care and failing to safeguard and protect Plaintiff's and the other Class Members' PII.

106. It was reasonably foreseeable that Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class Members' PII would result in an unauthorized third-party gaining access to such information for no lawful purpose.

107. As a direct result of Defendants' breach of their duty of confidentiality and privacy and the disclosure of Plaintiff's and the member of the Class confidential information, Plaintiff and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, increased infiltrations into their privacy through spam and/or attempted identity theft, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

108. By engaging in the negligent acts and omissions alleged herein, which permitted an unknown third party to access Defendants' systems containing the PII at issue, Defendants failed to meet the data security standards set forth under Section 5 of the FTC Act, which prohibits "unfair…practices in or affecting commerce." This prohibition includes failing to have adequate data security measures, which Defendants have failed to do as discussed herein.

109. Defendants' failure to meet this standard of data security established under Section 5 of the FTC Act is evidence of negligence.

110. Neither Plaintiff nor other Class Members contributed to the Data Breach as described in this Complaint.

111. Plaintiff's and the other Class members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiff and the other Class members are entitled to nominal damages.

112. Defendants' wrongful actions and/or inaction and the resulting Breach (as described above) constituted (and continue to constitute) negligence at common law.

/ / /

/ / /

/ / /

/ / /

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

COUNT IV
INVASION OF PRIVACY BY PUBLIC DISCLOSURE OF PRIVATE FACTS
(On behalf of Plaintiff and the Nationwide Class or, alternatively, the Texas Subclass)

113. The preceding factual statements and allegations are incorporated herein by reference.

114. Plaintiff's and the other Class Members' PII was (and continues to be) sensitive and personal private information.

115. By virtue of Defendants' failure to safeguard and protect Plaintiff's and the other Class Members' PII and the resulting Breach, Defendants wrongfully disseminated Plaintiff's and the other Class Members' PII to unauthorized persons.

116. Dissemination of Plaintiff's and the other Class Members' PII is not of a legitimate public concern; publicity of their PII was, is and will continue to be offensive to Plaintiff, the other Class Members and all reasonable people. The unlawful disclosure of same violates public mores.

117. As a direct result of Defendants' breach of their duty of confidentiality and privacy and the disclosure of Plaintiff's and the member of the Class confidential information, Plaintiff and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, increased infiltrations into their privacy through spam and/or attempted identity theft, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

118. Plaintiff and the other Class members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PII; (iii) loss of privacy; (iv) out-of-pocket expenses

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiff and the other Class Members are entitled to nominal damages.

119. Defendants' wrongful actions and/or inaction and the resulting Breach (as described above) constituted (and continue to constitute) an invasion of Plaintiff's and the other Class Members' privacy by publicly and wrongfully disclosing their private facts (*i.e.*, their PII) without their authorization or consent.

COUNT V
BREACH OF FIDUCIARY DUTY OF CONFIDENTIALITY
(On behalf of Plaintiff and the Nationwide Class or, alternatively, the Texas Subclass)

120. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

121. At all times during Plaintiff's and Class Members' interactions with Defendants as their customers, Defendants were fully aware of the confidential and sensitive nature of Plaintiff's and the Class Members' PII that Plaintiff and Class Members provided to Defendants.

122. Plaintiff's and Class Members' PII constitutes confidential and novel information. Indeed, Plaintiff's and Class Members' Social Security numbers can be changed only with great difficulty and time spent, which still enables a threat actor to exploit that information during the interim; additionally, an individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventative action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual ongoing fraudulent activity to obtain a new number.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

123. As alleged herein and above, Defendants' relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff's and Class Members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

124. Plaintiff and Class Members provided their respective PII to Defendants with the explicit and implicit understandings that Defendants would protect and not permit the PII to be disseminated to any unauthorized parties.

125. Defendants voluntarily received in confidence Plaintiff's and Class Members' PII with the understanding that the PII would not be disclosed or disseminated to the public or any unauthorized third parties.

126. Due to Defendants' failure to prevent, detect, and avoid the Data Breach from occurring by, *inter alia*, not following best information security practices and by not providing proper employee training to secure Plaintiff's and Class Members' PII, Plaintiff's and Class Members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

127. As a direct and proximate cause of Defendants' actions and/or omissions, Plaintiff and Class Members have suffered damages.

128. But for Defendants' disclosure of Plaintiff's and Class Members' PII, in violation of the parties' understanding of confidentiality, Plaintiff's and Class Members' PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendants' Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' PII, as well as the resulting damages.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

129. The disclosure of Plaintiff's and Class Members' PII constituted a violation of Plaintiff's and Class Members' understanding that Defendants would safeguard and protect the confidential and novel PII that Plaintiff and Class Members were required to disclose to Defendants.

130. The concrete injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiff's and Class Members' PII. Defendants knew their data security procedures for accepting and securing Plaintiff's and Class Members' PII had numerous security and other vulnerabilities that placed Plaintiff's and Class Members' PII in jeopardy.

131. As a direct and proximate result of Defendants' breaches of confidence, Plaintiff and Class Members have suffered and/or are at a substantial risk of suffering from damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiff and the other Class Members are entitled to nominal damages.

COUNT VI
NEGLIGENT TRAINING AND SUPERVISION
(On behalf of Plaintiff and the Nationwide Class or, alternatively, the Texas Subclass)

132. The preceding factual statements and allegations are incorporated herein by reference.

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

133. At all times relevant hereto, Defendants owe a duty to Plaintiff and the Class to hire competent employees and agents, and to train and supervise them to ensure they recognize the duties owed to their customers.

134. Defendants breached their duty to Plaintiff and the member of the Class by allowing their employees and agents to give access to customer PII to unauthorized users.

135. As a direct result of Defendants' breach of their duty of confidentiality and privacy and the disclosure of Plaintiff's and the member of the Class confidential information, Plaintiff and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, increased infiltrations into their privacy through spam and/or attempted identity theft, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

136. Plaintiff and the other Class members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiff and the other Class Members are entitled to nominal damages.

137. Defendants' wrongful actions and/or inaction and the resulting Breach (as described above) constituted (and continue to constitute) an invasion of Plaintiff's and the other Class Members' privacy by publicly and wrongfully disclosing their private facts (*i.e.*, their PII) without their authorization or consent.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

COUNT VII
BREACH OF COVENANT OF GOOD FAITH AND FAIR DEALING
(On behalf of Plaintiff and the Nationwide Class or, alternatively, the Texas Subclass)

138. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

139. As described above, when Plaintiff and the Class Members provided their PII to Defendants, they entered into implied contracts in which Defendants agreed to comply with their statutory and common law duties and industry standards to protect Plaintiff's and Class Members' PII and to timely detect and notify them in the event of a data breach.

140. These exchanges constituted an agreement between the parties: Plaintiff and Class Members were required to provide their PII in exchange for products and services provided by Defendants as well as an implied covenant by Defendants to protect Plaintiff's PII in their possession.

141. It was clear by these exchanges that the parties intended to enter into an agreement. Plaintiff and Class Members would not have disclosed their PII to Defendants but for the prospect of Defendants' promise of certain products and services. Conversely, Defendants presumably would not have taken Plaintiff's and Class Members' PII if it did not intend to provide Plaintiff and Class Members with the products and services it was offering.

142. Implied in these exchanges was a promise by Defendants to ensure that the PII of Plaintiff and Class Members in their possession was only used to provide the agreed-upon products and services.

143. Plaintiff and Class Members therefore did not receive the benefit of the bargain with Defendants, because they provided their PII in exchange for Defendants' implied agreement to keep it safe and secure.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

144. While Defendants had discretion in the specifics of how they met the applicable laws and industry standards, this discretion was governed by an implied covenant of good faith and fair dealing.

145. Defendants breached this implied covenant when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and regulations. These acts and omissions included: omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiff's and Class Members' PII; storing the PII of former customers, despite any valid purpose for the storage thereof having ceased upon the termination of the business relationship with those individuals; and failing to disclose to Plaintiff and Class Members at the time they provided their PII to it that Defendants' data security systems failed to meet applicable legal and industry standards.

146. Plaintiff and Class Members did all or substantially all the significant things that the contract required them to do.

147. Likewise, all conditions required for Defendants' performance were met.

148. Defendants' acts and omissions unfairly interfered with Plaintiff's and Class Members' rights to receive the full benefit of their contracts.

149. Plaintiff and Class Members have been or will be harmed by Defendants' breach of this implied covenant in the many ways described above, including actual identity theft and/or imminent risk of certainly impending and devastating identity theft that exists now that cyber criminals have their PII, and the attendant long-term expense of attempting to mitigate and insure against these risks.

150. Defendants are liable for their breach of these implied covenants, whether or not it is found to have breached any specific, express contractual term.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
SJG
STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

151. Plaintiff and Class Members are entitled to damages, including compensatory damages and restitution, declaratory and injunctive relief, and attorneys' fees, costs, and expenses.

COUNT VIII
DECLARATORY AND INJUNCTIVE RELIEF
(On behalf of Plaintiff and Nationwide Class, or, alternatively, the Texas Subclass)

152. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

153. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. § 2201.

154. As previously alleged, Plaintiff and Class Members entered into an implied contract that required Defendants to provide adequate security for the PII it collected from Plaintiff and Class Members.

155. Defendants owe a duty of care to Plaintiff and Class Members requiring it to adequately secure their PII.

156. Defendants still possess Plaintiff's and Class Members' PII.

157. Since the Data Breach, Defendants have announced few, if any, changes to their data security infrastructure, processes, or procedures to fix the vulnerabilities in their computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent future attacks.

158. Defendants have not satisfied their contractual obligations and legal duties to Plaintiff and Class Members, in fact, now that Defendants' insufficient data security is known to hackers, the PII in Defendants' possession is even more vulnerable to cyberattack.

159. Actual harm has arisen in the wake of the Data Breach regarding Defendants' contractual obligations and duties of care to provide security measures to Plaintiff and Class

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their PII and Defendants' failure to address the security failings that led to such exposure.

160. There is no reason to believe that Defendants' security measures are any more adequate now than they were before the Data Breach to meet Defendants' contractual obligations and legal duties.

161. Plaintiff, therefore, seeks a declaration (1) that Defendants' existing security measures do not comply with their contractual obligations and duties of care to provide adequate security, and (2) that to comply with their contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendants audit, test, and train their security personnel regarding any new or modified procedures;

d. Ordering that Defendants segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' systems is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. Ordering that Defendants purge, delete, and destroy in a reasonably secure manner customer data not necessary for their provisions of services;

f. Ordering that Defendants conduct regular computer system scanning and security checks;

g. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

h. Ordering Defendants to meaningfully educate their current, former, and prospective customers about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Petition, respectfully request that the Court enter judgment in their favor and against Defendants, as follows:

A. Declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiff as Class Representatives and appointing Plaintiff's counsel as Lead Counsel for the Class;

B. Declaring that Defendants' conduct was extreme and outrageous;

C. Declaring that Defendants breached their implied contract with Plaintiff and Class Members;

D. Declaring that Defendants negligently disclosed Plaintiff's and the Class Members PII;

E. Declaring that Defendants have invaded Plaintiff's and Class Members' privacy;

F. Declaring that Defendants breached their implied contract with Plaintiff and the Class Members;

G. Declaring that Defendants were negligent by negligently training and supervising their employees and agents;

H. Ordering Defendants to pay actual damages to Plaintiff and the Class Members;

I. Ordering Defendants to properly disseminate individualized notice of the Breach to all Class Members;

J. For an Order enjoining Defendants from continuing to engage in the unlawful business practices alleged herein;

K. Ordering Defendants to pay attorneys' fees and litigation costs to Plaintiff;

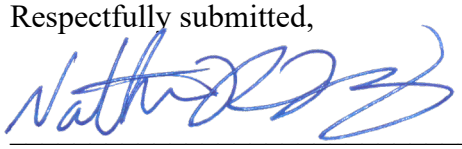
L. Ordering Defendants to pay both pre- and post-judgment interest on any amounts awarded; and

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

M. Ordering such other and further relief as may be just and proper.

Date Submitted: September 27, 2023

Respectfully submitted,



Nathan R. Ring
Nevada State Bar No. 12078
STRANCH, JENNINGS & GARVEY, PLLC
3100 W. Charleston Blvd., Ste. 208
Las Vegas, NV 89102
Telephone: 725-235-9750
E-mail: LasVegas@StranchLaw.com

Maureen M. Brady MO #57800
(pro hac vice petition forthcoming)
MCSHANE & BRADY, LLC
1656 Washington Street, Suite 120
Kansas City, MO 64108
Telephone: (816) 888-8010
Facsimile: (816) 332-6295
E-mail: mbrady@mcshanebradylaw.com

Sharon J. Zinns, Esq.
(pro hac vice petition forthcoming)
Georgia Bar No. 552920
ZINNS LAW, LLC
4243 Dunwoody Club Drive, Suite 104
Atlanta, GA 30350
(404) 882-9002
sharon@zinnslaw.com

Attorneys for Plaintiffs